ABSTRACT

A cryptosystem has a secret based on an order of a group of points on a Jacobian of a curve. In certain embodiments, the cryptosystem is used to generate a product identifier corresponding to a particular product. The product identifier is generated by initially receiving a value associated with a copy (or copies) of a product. The received value is padded using a recognizable pattern, and the padded value is converted to a number represented by a particular number of bits. The number is then converted to an element of the Jacobian of the curve, and the element is then raised to a particular power. The result of raising the element to the particular power is then compressed and output as the product identifier. Subsequently, the encryption process can be reversed and the decrypted value used to indicate validity and/or authenticity of the product identifier.